11-30-2010

Micro-Blogging in the Workplace

Chia Yao Lee
Deakin University

Matthew Warren
Deakin University

DOI: 10.4225/75/57b6722a3477e
8th Australian Information Security Mangement Conference, Edith Cowan University, Perth Western Australia, 30th November 2010

Micro-Blogging in the Workplace

Chia Yao Lee and Matthew Warren
School of Information Systems
Deakin University
Melbourne, Australia
chia.lee@deakin.edu.au

Abstract

Micro-blogging services such as Twitter, Yammer, Plurk and Google Buzz have generated substantial interest among members of the business community in recent years. Many CEOs, managers and front-line employees have embraced micro-blogs as a tool for interacting with colleagues, employees, customers, suppliers and investors. Micro-blogs are considered a more informal channel than emails and official websites, and thus present a different set of challenges to businesses. As a positional paper, this paper uses a case study of a bogus Twitter account to emphasise security and ethical issues relating to (i) Trust, Accuracy and Authenticity of Information, (ii) Privacy and Confidentiality, and (iii) Scams and Frauds, when micro-blogs are used in the workplace. It also highlights the potential risks businesses are exposed to if employees use micro-blogs irresponsibly. The paper contributes to practice by providing suggestions on managing security and ethical risks associated with micro-blogging in the workplace. It contributes to research by building on existing research in trust and data privacy in electronic communication.

Keywords

Micro-blogs, privacy, confidentiality, security, trust.

INTRODUCTION

The former Prime Minister of Australia, Kevin Rudd, was and still is an active user of Twitter. His thoughts on policy matters and community issues were posted on his Twitter stream regularly. Social activities he undertook with his family were also included in his Twitter stream, for instance, the movies he brought his boys to, and the occasional shopping trip he accompanied his wife on. Even after Kevin Rudd was replaced as Australia's Prime Minister, he updated his Twitter followers regularly on his movements and plans. There was little doubt that Twitter was used both as a formal and informal channel of communication by Kevin Rudd to reach out to electorates.

Other well known individuals who are prolific users of micro-blogs include Bill Gates, Lance Armstrong and Ashton Kutcher. It comes as no surprise that micro-blogs have become the communication channel of choice for politicians, celebrities and sports stars wishing to interact with their supporters and fans directly. Micro-blog postings do not require the same effort required for writing a full-fledged blog entry, which is more akin to writing thought pieces and columns in newspapers. Micro-blogging is no longer a communication channel that is exclusive to politicians and well known individuals; students and educators, business executives and housewives have all embraced micro-blogging. The fact that Facebook, an online social network with over 500 million users, supports micro-blogging through its status update function suggests that there are no less than half a billion micro-bloggers globally as of July 2010 (Zuckerberg 2010).

As a supplementary channel for communication, micro-blogs have become a popular tool for marketing. When Virgin America airways launched their new California-Toronto flights, they invited key influencers in the blogosphere to mention the new routes on their Twitter streams in return for discounted flights rather than spending extensively on traditional media advertising (Leo 2010). Apart from marketing, businesses have used micro-blogs to handle customer complaints and for obtaining customer input when developing new products.

The previous examples demonstrate the effectiveness of micro-blogs as a communication tool for interacting with internal and external stakeholders, for formal and informal communication. However, the use of micro-blogs has generated substantial negative publicity when celebrities and athletes posted controversial messages and content on micro-blogs. Well known athletes and film stars have lost lucrative sponsorship contracts or film opportunities due to inappropriate micro-blog postings (ABC 2010).

When used in the workplace micro-blogs may expose businesses and their employees to new security and ethical risks. Using a case study of a fake Twitter account by a former Telstra employee, this paper discusses important security and ethical implications relating to the use of micro-blogs in the workplace. As a positional paper, the paper emphasises the unique characteristics of micro-blogs which make it extremely challenging for employers to regulate micro-blogging in the workplace. The analysis of the fake Twitter account case provides a basis for understanding security and ethical

issues that arise when micro-blog accounts are compromised, if micro-blog postings are hijacked; and the difficulties associated with verifying the validity and accuracy of micro-blog postings, and authenticating the identity of micro-bloggers.

A survey by Proofpoint (Goodchild 2010) found that Twitter was mentioned by 17 per cent of respondents as a source of investigation due to exposure of sensitive, confidential and private information. Many respondents in the Proofpoint survey also indicate their awareness of security risks associated with Twitter scams (Goodchild 2010). This paper was motivated primarily by the severity of security and ethical issues concerning micro-blog use for work, and at work. For example, how should employees be regulated when they use their personal micro-blog accounts to interact with customers, or how would employees be restricted from mentioning personal and non-work related information when micro-blogging in their official capacity due to the social nature of micro-blogs. Many micro-blog followers have been attracted to the new channel due to the informal and social aspect of the channel in linking the micro-blogger directly with their contacts and followers. The paper explores issues such as whether employers should formulate policies specific to micro-blog use, or could a more generic policy on all forms of electronic communications suffice in addressing a broader range of security and ethical threats for social media (Lee 2009).

The paper is organised as follows. Section 2 of the paper presents an overview and description of micro-blogs, comparing them to emails, SMS text messages and other forms of electronic communications. Section 3 presents the case study of a bogus micro-blog account. Section 4 discusses the business implication of micro-blogs on trust, confidentiality, privacy, security and business ethics. Section 5 discusses the contributions of the paper and directions for future research.

LITERATURE REVIEW

Micro-blog services such as Twitter, Yammer, Plurk and Emote enable micro-blog users to post 140 character-long messages which could then be accessed by their followers. Some users restrict access to their micro-blog streams whereas others make theirs accessible to the public. The format of micro-blog postings has evolved, with several micro-blog services also supporting multimedia attachments and URL links. Online social networks such as Facebook support micro-blogging through the user status update function. Google has recently introduced Google Buzz, a new functionality within Gmail that enables users to post micro-blog-like status updates, and Microsoft's Windows Live Messenger provides a similar status update micro-blogging function.

As a mass communication channel, micro-blogs are not edited by reviewers or editors prior to publication. Unlike a full-fledged online diary or weblog, micro-blog entries are short and swift. Micro-blogs are a transparent, one-to-many online conversational platform. Users could post micro-blog entries through web browsers, web-based applications, mobile applications, or via emails and SMS text messages. Followers of micro-blogs could post a reply to a micro-blog entry, or repost the original micro-blog entry in their own micro-blog stream as a re-tweet. Although micro-blogs are often compared to SMS text messages, micro-blogs are relatively more effective that the former when used for reaching multiple followers simultaneously. Unlike SMS text messages, micro-blog followers have a choice of whether to subscribe to a micro-bl

Many micro-blog services enable users to "hash-tag" postings so that their micro-blogs could be indexed and searched by other users according to hash-tagged keywords. An aggregation of hash-tags could then be used to monitor trends in micro-blog postings (Java et al. 2007). In recent times, social commentators and media have relied on trending hash-tags in micro-blogs to follow development of important events in real-time, such as the launch of Apple's iPad in April 2010, and the Qantas A380 engine malfunction in Singapore in November 2010.

In an enterprise environment, micro-blogs are in many ways similar to emails, instant messaging, online forums and other forms of electronic communication. However, micro-blogs stand out in that they enable short postings to be tagged and indexed, thus be made searchable by users according to keywords and context. Access to micro-blog streams could also be configured to private or public, giving the micro-blogger a convenient way for controlling access to their micro-blog postings (Oliver et al 2009). Furthermore, when third party micro-blogging services like Twitter and Yammer are used in the workplace, businesses do not have full control over the provision of the service and the underlying security mechanisms. In contrast, email services are often hosted internally within the organisation. Emails are typically used for private communication between two parties, and not as often for mass-communication (e.g. email lists, subscription) due substantial difficulty in assessing whether mass emails are viewed as spam or unsolicited communication by recipients. In comparison, followers of micro-blogs could subscribe to specific micro-blog streams, and sort micro-blog entries according to a wide range of parameters, e.g. the micro-blog contributors, keyword tags, date and time, and more recently, geographical tags, thus giving the recipient greater control in determining what postings they follow.

Micro-blogs are often treated as a more informal communication channel due to the way micro-blog postings are made. With a limitation of 140 characters, micro-bloggers are encouraged to write in short-hand, much like in SMS text messages, thus explaining the more informal language used. The ability to post micro-blog entries on mobile devices encourages micro-bloggers to post entries or respond to entries in real-time, often when they are not seated in front of a computer and a desk.

Regulation of micro-blogging in the workplace varies. Xerox for example, developed social media guidelines that require employees to outline clearly the business purpose of engaging social media, acknowledge understanding of the guidelines, and confirm managerial support. Once such a request has been reviewed, a formal confirmation is provided (Wreden 2010). In contrast, Mel-O-Cream Donuts have stated that they do not require specific policies on social media use. Employees are trusted to act responsibly and do what is best for the company. Acceptable activities are communicated through employee orientation processes, meetings, corporate newsletters and handbook (Wreden 2010). The Australian Public Service Commission published the "Protocols for Online Media Participation" in 2009 (APS 2009), and the Department of Finance and Deregulation in Australia published a guideline on social media use by staff in 2010 (AGIMO 2010), suggesting that whilst concerned with social media use by employees, private and public organisations are adopting a broader social media policy for regulating micro-blog use in the workplace.

THE CASE OF THE BOGUS TWITTER ACCOUNT

A former Telstra employee, Leslie Nassar impersonated Communications Minister Stephen Conroy on Twitter and made comments as if they were from the minister. This impersonation took the form of setting up a Twitter account and posting under the Twitter name http://twitter.com/stephenconroy.

The government response to the bogus Twitter account was "The real Stephen Conroy is aware of the fake Stephen Conroy, and he doesn't have his own presence on Twitter. Satire is an important part of any healthy democracy. There are many social-networking platforms available through which ministers can communicate, and we haven't made a decision on whether or which one should be the way to go." (Sydney Morning Herald 2009a). The bogus Twitter story was reported widely in the press, some social media organisations ran stories trying to identify the identity of the bogus micro-blogger e.g. a list of the top twenty five suspects (including Stephen Conroy) (Amensia Blog 2009). A screen shot of the bogus Twitter account is shown in Figure 1.

Figure 1: Screenshot of the bogus Stephen Conroy Twitter account

Nassar announced on the 16th March, 2009 that he was the person behind the fake Twitter account. On the 17th March, 2009 the fake Twitter account was closed (it was not clear who closed the account). Nassar had published 708 tweets and attracted 1531 followers, his tweets related to the proposed Australian Federal Government measures to filter Internet content (Sydney Morning Herald 2009b).

Aftermath

Nassar wrote the Twitter posts as a completely separate endeavour to his work at Telstra. The issue became a political one, because of the tensions between Telstra and the Australian Federal Government, which has excluded Telstra from the bidding process to build a $10 billion-plus National Broadband Network (Sydney Morning Herald 2009c).

Interviews with Nassar, identified that he did not create the original Stephen Conroy account but took it over. The interviews with Nassar also highlighted that when he went public over his identity, he was put under pressure by his Telstra managers to close the fake Stephen Conroy Twitter account (ZdNET 2009a). Nassar posted his views online regarding his treatment by Telstra Management on the 26th March, 2009 (ZdNET 2009b) and according to Nassar he was then officially sacked by Telstra on 26th March (ABC 2009a).

Telstra's Response

Telstra's response only occurred after the 16th March when Nassar's identity was made public. On the 26th March, Telstra announced it had undertook "disciplinary" action against Nassar, according to Telstra, not because of his Fake Stephen Conroy Twitter posts but because of his ongoing unauthorised public statements about Telstra, including abusive comments towards a Telstra employee (Sydney Morning Herald 2009d).

In response, in April, 2009, Telstra announced the launch of a new Telstra social media policy - Social Media - Telstra's 3 Rs of Social Media Engagement (Telstra 2009). In brief, the Telstra 3 Rs (Representing, Responsibility and Respect) Policy asked Telstra staff that when engaging in social media they must be clear about who they are representing, that they take responsibility for ensuring that references to Telstra are factually correct and accurate and do not breach confidentiality requirements, and that Telstra show respect for the individuals and communities with which they interact. It is important to note that this policy does not apply to Telstra employees' personal use of social media platforms where the employee makes no reference to Telstra related issues (Telstra 2009). The policy also defines that Telstra staff should disclose only publicly available information and that they must not comment on or disclose confidential Telstra information (Telstra 2009).

The Telstra policy may not have stopped the bogus Stephen Conroy Twitter incident, but clearly defines the responsibilities of Telstra employees. An interesting aspect of the policy which still remains unproven is whether an organisational policy would control Telstra staff behaviour in their personal, non-work time.

DISCUSSION OF IMPLICATIONS

The case study above highlights several security and ethical issues relating to the use of micro-blogs in the workplace. This section provides a discussion of three specific issues, namely (i) trust, accuracy and authenticity, (ii) privacy and confidentiality, (iii) scams and frauds.

Trust, Accuracy and Authenticity

The establishment of an official micro-blog account for a business does not undergo the same levels of checks and verification as the registration of a legal company name or trademark, or even those required for registering a domain name for an Internet website. An individual could select usernames and profiles that lead followers to believe that the micro-blog account belongs to another user or company. Often, micro-blog users will post a thumbnail photo of themselves, or a company logo to help identify themselves, but unless the owner of the photo or logo are actively searching for unauthorised use of their images, there is very little that other users could do to verify the identity of a micro-blogger. In the case study above, a picture of Senator Conroy was used, although the label "Dead Stephen Conroy" is a clue that the account is bogus. The ability to register usernames anonymously on micro-blogging platforms has given rise to username "squatters" who will register the names of celebrities or well known persons.

The other issue with trust, accuracy and authenticity relates to the weakness of security mechanisms in place for detecting and restoring micro-blog accounts which have been hijacked or compromised. Phishing attacks, malicious wares, keyloggers, scams and social engineering frauds are simple mechanisms which could be used to lure legitimate micro-blog users into revealing username and password combinations to hackers. Once a micro-blog account or profile has been compromised, there is little that a micro-blog follower could do to verify the authenticity of each micro-blog post, or to verify the identity of the user controlling the account. Although the developers and operators of micro-blog services, e.g. Twitter, Google, Facebook, have a responsibility in shutting down fake accounts, and restoring compromised accounts, substantial damages could be done in the interim, and followers of micro-blogs may be misled by fake postings. The ease of registering http://twitter.com/stephenconroy and compromising the Twitter account

highlight a need to ensure that identification checks are put in place to prevent the creation of fake and misleading profiles.

In response to the large number of fake Twitter accounts, and reaction to a lawsuit due to fake tweets, Twitter has introduced a beta "Verified Accounts" program in mid-2009 (Katz 2009) for well known micro-bloggers (Twitter 2010). Verified accounts will show a verified badge next to the Twitter profile to identify users who have been verified. The beta program has been discontinued as of September 2010 (Twitter 2010).

As micro-blogs have a potential in influencing public sentiments and causing libellous damage to businesses, the question that begs to be answered is what level of security is suitable for creating micro-blog accounts and posting micro-blog messages. Should an encrypted, secure login session similar to those used for online banking be used for identity-verified micro-blog accounts?

Privacy and Confidentiality

The case study has illustrated several problems businesses face if employees use micro-blogs to discuss commercial-in-confidence information. There is a risk of leakage of confidential and private information as micro-blogs are designed primarily as an information exchange and dissemination tool. Once confidential and private data is discussed in micro-blogs, there is the risk of a recipient or subscriber of a Tweeter stream re-tweeting the posting, and spreading the confidential information to others. Unlike emails which were designed for transmitting information between well defined individuals, micro-blogs were designed for circulating information publicly in an efficient and effective manner.

To encrypt micro-blog postings like secure emails, or to put security stamps to ensure confidentiality may defeat the primary function of micro-blogs, which is to disseminate information quickly and effectively. Furthermore, the lack of awareness and complexity in setting security configurations for micro-blogs makes the issue of limiting access, securing logins and postings more difficult for the majority of micro-bloggers.

Whilst micro-bloggers may have received specific directions from employers that restrict them from mentioning confidential and private work information on micro-blogs, little can be done to stop users from posting their personal thoughts, social activities and hobbies on micro-blogs. Users could inadvertently allow other users to collect and re-combine rich profile information from micro-blog postings to prepare for a targeted attack on an individual, e.g. identity theft and cyber stalking. In the case study above, the user behind the fake Twitter account could have solicited information from other users if the credentials of fake account manage to fool real-life friends and contacts of Stephen Conroy's.

At present, many businesses do not have formal policies on social media use, thus it is almost impossible for businesses to stop their employees from falsely representing the business in soliciting private and confidential data from business partners, if not leak these important data to adversaries through micro-blogs.

Scams and Frauds

Directly related to the issue of trust, authenticity of users and postings, and the leak of private and confidential data is the issue of online scams and frauds. Although micro-blogging services do not handle financial transactions and payments, identity fraud, scams, and phishing attacks on micro-blogging services are not unheard of. The hijacking of micro-blog accounts could be used for more heinous criminal activities, such as stalking, online bullying, and identity theft.

Unlike online banking services which have several layers of security mechanisms, micro-blogging sites are often simple, and the default security settings have been left in the least secure level until a reasonably knowledgeable user modifies the security settings. Consequently, micro-blogging services may evolve into a means for identity theft due to the richness of the data posted by users, the temporal and spatial relevance of the data, and the relationship formed between a user and his/her contacts.

Scams and identity frauds will continue to take place through micro-blogs until a quicker and more effective way for shutting down fake profiles and bogus accounts is introduced. Otherwise fraudsters will continue to have a headstart. Fake Facebook pages and Twitter account will only be shutdown when sufficient evidence have been collected, or after substantial damages have taken place. The ability for online social networks and micro-blogging services to support third party applications (apps) will also complicate matters in terms of the protection of users against online scams and frauds propagated through third party apps that extract content from micro-blogs.

Training and educating employees to increase their awareness of security threats is perhaps the only effective method available to employers. For instance, the emergence of a Twitter "javascript mouseover" hack on 22 September 2010 illustrates the ease for micro-blogging sites to be compromised. Unless employees are aware and up-to-date with developments in micro-blogging, those who place their computer cursors over a hyperlink on Twitter's website would have their Internet browsers taken over, and an unauthorised website accessed (Sydney Morning Herald 2010).

CONCLUSION

As more businesses adopt micro-blogs to supplement traditional communication channels for internal and external communication, more resources will have to be allocated by businesses to identify and address the security and ethical threats associated with micro-blogging. The introduction of guidelines and policies specific to micro-blogging may be pre-mature at this point in time as micro-blogging services continue to evolve. On the contrary, guidelines and policies that encourage intelligent and correct use of electronic communications and social media may provide a more robust framework for countering security and ethical threats associated with micro-blogging. Furthermore, businesses may have little choice but to "stake their flag" in the micro-blogosphere to ensure that their trademarks and identifying characteristics have not been hijacked by imposters and identity thieves.

The study contributes to practice by providing suggestions on managing security and ethical risks associated with micro-blogging in the workplace. It contributes to research by building on current research in trust and data privacy in electronic communication. The study also presents several suggestions for future research, for instance, an analysis of social media policies in businesses, an evaluation of organisational practice relating to micro-blog use, a survey of user awareness of micro-blogging security issues, and an analysis of methods for protecting users from fraudulent and compromising activities associated with micro-blogging.

REFERENCES

ABC (Australian Broadcasting Corporation) (2009) Telstra fired me: fake Stephen Conroy, URL: http://www.abc.net.au/news/stories/2009/03/26/2526650.htm, Accessed 1st September, Accessed 1st September 2010.

ABC (Australian Broadcasting Corporation) (2010) Jaguar dumps Rice after Twitter slur, URL: www.abc.net.au/news/stories/2010/09/07/3004765.htm, Accessed 1st September, Accessed 1st September 2010.

AGIMO (Australian Government Information Management Office) (2010) Social Media 101: A beginner's guide for Finance employees, URL: http://agimo.govspace.gov.au/files/2010/04/social-media-101.pdf, Accessed 1st November 2010.

Amensia Blog (2009) Who is Fake Stephen Conroy? Full list of Suspects, 9th March, URL http://amnesiablog.wordpress.com/2009/03/09/who-is-fake-stephen-conroy-full-list-of-suspects, Accessed 1st September 2010.

APS (Australian Public Service Commission) (2009) Circular 2009/6: Protocols for online media participation, 18th November, URL: http://www.apsc.gov.au/circulars/circular096.htm, accessed 1st November 2010.

Goodchild, J. (2010) Survey: Fear of data loss, security risks via social media sites on the upswing, 20th September, URL: http://csoonline.com/article/print/616218, Accessed 1st September 2010.

Gunther, O., Krasnova, H., Richle, D., and Schondienst, V. (2009) Modeling Microblogging Adoption in the Enterprise, Proceedings of the Fifteenth Americas Conference on Information Systems (AMCIS), Ca., USA.

Java, A., Song, X., Finn, T., and Tseng, B. (2007) Why We Twitter: Understanding Microblogging Usage and Communities, Proceedings of the Joint 9th WEBKDD and 1st SNA-KDD Workshop 2007, Ca., USA.

Katz, L. (2009) Twitter to roll out 'Verified Accounts' this summer, CNET News, URL: http://news.cnet.com/8301-1023_3-10258816-93.html, Accessed 1st September 2010.

Lee, C. Y. (2009) Understanding Security Threats in Virtual Worlds, Proceedings of the Fifteenth Americas Conference on Information Systems (AMCIS), Ca. USA.

Leo, J. (2010) Twitter your way to a free Toronto ticket on Virgin America, LA Times, Daily Travel and Deal Blog, URL: http://travel.latimes.com/daily-deal-blog/index.php/twitter-your-way-to--6789/, Accessed 1st September 2010.

Sydney Morning Herald (2009a) Connection more trick than tweet, 9th March, URL: http://www.smh.com.au/national/connection-more-trick-than-tweet-20090306-8rd5.html, Accessed 1st September 2010.

Sydney Morning Herald (2009b) Telstra man behind Fake Stephen Conroy, 17th March, URL: http://www.smh.com.au/articles/2009/03/17/1237054799469.html, Accessed 1st September 2010.

Sydney Morning Herald (2009c) Fake Stephen Conroy lashes out at Telstra, 18th March, URL: http://www.smh.com.au/articles/2009/03/18/1237054872141.html, Accessed 1st September 2010.

Sydney Morning Herald (2009d) Fake Stephen Conroy's 'fake' sacking, 26th March, URL: http://www.smh.com.au/news/home/technology/fake-stephen-conroys-fake-sacking/2009/03/26/1237657035076.html, Accessed 1st September 2010.

Sydney Morning Herald (2010) Twitter hack opens popups, causes havoc, 22nd September, URL: http://www.smh.com.au/technology/technology-news/twitter-hack-opens-popups-causes-havoc-20100922-15lns.html, Accessed 22nd September 2010.

Telstra (2009) Social Media - Telstra's 3 Rs of Social Media Engagement, URL: http://www.telstra.com.au/abouttelstra/download/document/social-media-company-policy-final-150409.pdf, Accessed 1st September 2010.

Twitter (2010) About Verified Accounts, Twitter Help Center / Twitter basics, URL: http://support.twitter.com/groups/31-twitter-basics/topics/111-features/articles/119135-about-verified-accounts, Accessed 1st September 2010.

Wreden, N. (2010) Social Media Policies for Business, IT Management – Baseline, URL: http://www.baselinemag.com/c/a/IT-Management/Social-Media-Policies-for-Business-181423/, Accessed 1st September 2010.

ZdNET (2009a) Q&A: Leslie Nassar (Fake Stephen Conroy), March 22nd, URL: http://www.zdnet.com.au/q-a-leslie-nassar-fake-stephen-conroy-339295582.htm, Accessed 1st September 2010.

ZdNET (2009b) Fake Conroy abuses Telstra boss Bradlow, 26th March, URL: http://www.zdnet.com.au/fake-conroy-abuses-telstra-boss-bradlow-339295680.htm, Accessed 1st September 2010.

Zuckerberg, M. (2010) 500 Million Stories, The Facebook Blog, URL: http://blog.facebook.com/blog.php?post=409753352130, Accessed 1st September 2010.